PCT/JP2004/014996

05.10.2004

# 日本国特許庁
# JAPAN PATENT OFFICE



別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日
Date of Application: ２００３年１１月１１日

出願番号
Application Number: 特願２００３－３８０８４９

[ST. 10/C]: ［ＪＰ２００３－３８０８４９］

出願人
Applicant(s): 松下電器産業株式会社



２００４年１１月 ５日

特許庁長官
Commissioner,
Japan Patent Office

小川洋

出証番号 出証特２００４－３０９９９４９

【書類名】　特許願
【整理番号】　2048150033
【あて先】　特許庁長官殿
【国際特許分類】　G09C　1/00　640
【発明者】
　【住所又は居所】　大阪府門真市大字門真１００６番地　松下電器産業株式会社内
　【氏名】　庭野　智
【発明者】
　【住所又は居所】　大阪府門真市大字門真１００６番地　松下電器産業株式会社内
　【氏名】　徳田　克己
【発明者】
　【住所又は居所】　大阪府門真市大字門真１００６番地　松下電器産業株式会社内
　【氏名】　三浦　康史
【特許出願人】
　【識別番号】　000005821
　【氏名又は名称】　松下電器産業株式会社
【代理人】
　【識別番号】　100109210
　【弁理士】
　【氏名又は名称】　新居　広守
【手数料の表示】
　【予納台帳番号】　049515
　【納付金額】　21,000円
【提出物件の目録】
　【物件名】　特許請求の範囲　1
　【物件名】　明細書　1
　【物件名】　図面　1
　【物件名】　要約書　1
　【包括委任状番号】　0213583

【書類名】特許請求の範囲
【請求項１】
第１の情報提供者の提供する第１の情報と、第２の情報提供者から提供される前記第１の情報と関連する第２の情報を利用する端末装置において、
第３の情報で指定される情報提供者が署名した前記第２の情報を署名検証し利用可否判定する
ことを特徴とする情報利用可否判定方法。
【請求項２】
前記第１の情報が暗号化されている場合に、前記第３の情報が前記第１の情報の暗号鍵を含むライセンスに格納されている
ことを特徴とする請求項１記載の情報利用可否判定方法。
【請求項３】
前記第１の情報が暗号化されている場合に、前記第３の情報が暗号化された前記第１の情報に格納されている
ことを特徴とする請求項１記載の情報利用可否判定方法。
【請求項４】
前記第２の情報が暗号化されている場合に、前記第３の情報が暗号化された前記第２の情報の暗号鍵を含むライセンスに格納されている
ことを特徴とする請求項１記載の情報利用可否判定方法。
【請求項５】
前記第３の情報が、前記第１の情報提供者のみと、前記第１の情報提供者と前記第１の情報提供者が公開鍵証明書に署名した前記第２の情報提供者のみと、制限なし、のうちの少なくとも２つから１つを識別するフラグである
ことを特徴とする請求項２～請求項４のいずれか１項に記載の情報利用可否判定方法。
【請求項６】
前記第３の情報が、前記第２の情報の署名者を一意に特定する識別情報である
ことを特徴とする請求項２～請求項４のいずれか１項に記載の情報利用可否判定方法。
【請求項７】
前記端末装置に格納されている前記第１の情報提供者の公開鍵証明書を利用することで、前記第１の情報提供者が署名したと判断する
ことを特徴とする請求項５記載の情報利用可否判定方法。
【請求項８】
前記端末装置に格納されている前記第１の情報提供者を一意に特定する識別情報と前記第２の情報に含まれる署名者を一意に特定する識別情報が一致することで、前記第１の情報提供者が署名したと判断する
ことを特徴とする請求項５記載の情報利用可否判定方法。
【請求項９】
暗号化されている前記第１の情報に格納されている前記第１の情報提供者を一意に特定する識別情報と前記第２の情報に含まれる署名者を一意に特定する識別情報が一致することで、前記第１の情報提供者が署名したと判断する
ことを特徴とする請求項５記載の情報利用可否判定方法。
【請求項１０】
暗号化された前記第２の情報の暗号鍵を含む前記第２の情報のライセンスに含まれている前記第１の情報提供者を一意に特定する識別情報と前記第２の情報に含まれる署名者を一意に特定する識別情報が一致することで、前記第１の情報提供者が署名したと判断する
ことを特徴とする請求項５記載の情報利用可否判定方法。
【請求項１１】
前記端末装置で作成する前記第１の情報と関連する第４の情報に前記端末装置で作成したことを示す識別情報を格納し、前記第４の情報に前記端末装置で作成したことを示す識別情報を含む場合、前記第４の情報の署名検証を行わない

ことを特徴とする請求項２または請求項３記載の情報利用可否判定方法。
【請求項１２】
前記第４の情報の移動範囲指定情報を含む
ことを特徴とする請求項１１記載の情報利用可否判定方法。
【請求項１３】
暗号化された前記第１の情報に前記第４の情報の移動範囲指定情報を含む
ことを特徴とする請求項１１記載の情報利用可否判定方法。
【請求項１４】
前記第２の情報のライセンスに前記第４の情報の移動範囲指定情報を含む
ことを特徴とする請求項１１記載の情報利用可否判定方法。
【請求項１５】
前記第２の情報に前記第４の情報の移動範囲指定情報を含む
ことを特徴とする請求項１１記載の情報利用可否判定方法。
【請求項１６】
前記移動範囲指定情報が前記端末装置所有者の所有する前記端末装置に限定する場合に、前記第４の情報の少なくとも一部を前記端末装置所有者の所有する前記端末装置に共通の暗号鍵で暗号化する
ことを特徴とする請求項１２～請求項１５のいずれか１項に記載の情報利用可否判定方法。
【請求項１７】
前記第１の情報のライセンスに前記第４の利用可否情報を含む
ことを特徴とする請求項１６記載の情報利用可否判定方法。
【請求項１８】
暗号化された前記第１の情報に前記第４の利用可否情報を含む
ことを特徴とする請求項１６記載の情報利用可否判定方法。
【請求項１９】
第１の情報提供者の提供する暗号化された第１の情報と、第２の情報提供者から提供される前記第１の情報と関連する第２の情報を利用する端末装置において、
前記第１の情報の暗号鍵を含むライセンスに前記第２の情報を用いて前記第１の情報を利用することを指示する参照指示情報を含む
ことを特徴とする情報利用可否判定方法。
【請求項２０】
第１の情報提供者の提供する暗号化された第１の情報と、第２の情報提供者から提供される前記第１の情報と関連する第２の情報を利用する端末装置において、
暗号化された前記第１の情報に前記第２の情報を用いて前記第１の情報を利用することを指示する参照指示情報を含む
ことを特徴とする情報利用可否判定方法。
【請求項２１】
前記参照指示情報が前記第２の情報を用いるか否かを識別するフラグである
ことを特徴とする請求項１９または請求項２０記載の情報利用可否判定方法。
【請求項２２】
前記参照指示情報が前記第２の情報を一意に特定する識別情報である
ことを特徴とする請求項１９または請求項２０記載の情報利用可否判定方法。
【請求項２３】
前記参照指示情報が前記第２の情報の署名者を一意に特定する識別情報である
ことを特徴とする請求項１９または請求項２０記載の情報利用可否判定方法。
【請求項２４】
第１の情報提供者の提供する暗号化された第１の情報と、第２の情報提供者から提供される前記第１の情報と関連する第２の情報を利用する端末装置において、
前記第１の情報の暗号鍵を含むライセンスに前記第２の情報の編集可否情報を含む

ことを特徴とする情報利用可否判定方法。
【請求項２５】
第１の情報提供者の提供する暗号化された第１の情報と、第２の情報提供者から提供される前記第１の情報と関連する第２の情報を利用する端末装置において、
暗号化された前記第１の情報に前記第２の情報の編集可否情報を含む
ことを特徴とする情報利用可否判定方法。
【請求項２６】
第１の情報提供者の提供する暗号化された第１の情報と、第２の情報提供者から提供される前記第１の情報と関連する暗号化された第２の情報を利用する端末装置において、
暗号化された前記第２の情報の暗号鍵を含むライセンスに前記第２の情報の編集可否情報を含む
ことを特徴とする情報利用可否判定方法。
【請求項２７】
第１の情報提供者の提供する暗号化された第１の情報と、第２の情報提供者から提供される前記第１の情報と関連する第２の情報を利用する端末装置において、
前記第２の情報に前記第２の情報の編集可否情報を含む
ことを特徴とする情報利用可否判定方法。
【請求項２８】
前記編集可否情報が編集可能か否かを識別するフラグである
ことを特徴とする請求項２４～請求項２７のいずれか１項に記載の情報利用可否判定方法。
【請求項２９】
前記編集可否情報が前記第２の情報を一意に特定する識別方法である
ことを特徴とする請求項２４～請求項２７のいずれか１項に記載の情報利用可否判定方法。
【請求項３０】
前記編集可否情報が前記第２の情報の署名者を一意に特定する識別方法である
ことを特徴とする請求項２４～請求項２７のいずれか１項に記載の情報利用可否判定方法。
【請求項３１】
請求項１から請求項３０のいずれか１項に記載の情報利用可否判定方法により、前記第２の情報または前記第４の情報の利用可否を判定する前記端末装置を含むコンテンツ配信システム。

【書類名】明細書
【発明の名称】情報利用可否判定方法およびこの方法を用いたコンテンツ配信システム
【技術分野】
【０００１】
本発明は、放送または通信を用いて、映像、音楽などのデジタルコンテンツと、デジタルコンテンツのライセンスと、デジタルコンテンツの属性または制御情報などを含むメタデータを配信し、ユーザが端末装置でデジタルコンテンツを利用するシステムに関し、特に、メタデータの利用可否判定方法および利用可否判定方法を適用した装置を含むシステムに関する。
【背景技術】
【０００２】
デジタルコンテンツを提供するコンテンツプロバイダには、ＣＭスキップのためのシーンインデックスなど意図に反した不正なメタデータの流通を阻止したいという要求があり、メタデータを作成したメタデータプロバイダがメタデータに施すデジタル署名を用いて、不正なメタデータプロバイダを排除する方法が提案されている。
従来、特許文献１などに開示されているように、デジタル署名の検証を用いてメタデータの署名者の正当性とメタデータの中身の改ざんを検出し、メタデータの利用可否を判定している。
【０００３】
ここで、従来技術のデジタル署名によるメタデータの利用可否判定について説明する。メタデータのデジタル署名の検証には、デジタル署名されたメタデータと、メタデータ署名者の公開鍵証明書と、ＣＲＬ（Ｃｅｒｔｉｆｉｃａｔｅ　Ｒｅｖｏｃａｔｉｏｎ　Ｌｉｓｔ）を用いる。
ここで、メタデータへのデジタル署名は、コンテンツプロバイダ、または、メタデータプロバイダが行う。端末装置では、メタデータを利用する場合、次の手順でメタデータの利用可否判定を行う。
【０００４】
まず、メタデータにデジタル署名した署名者の署名者ＩＤがＣＲＬに含まれているか確認する。ここで、署名者ＩＤとは、署名者を一意に特定する識別情報である。
署名者ＩＤがＣＲＬに含まれている場合は、メタデータが利用不可と判定する。
署名者ＩＤがＣＲＬに含まれていない場合は、メタデータの署名を公開鍵証明書で検証し改ざん検出する。
【０００５】
改ざんが検出された場合は、メタデータが利用不可と判定する。
改ざんが検出されない場合は、メタデータが利用可能と判定する。
以上、従来技術のデジタル署名によるメタデータの利用可否判定について概略を説明した。
尚、デジタル署名の検証については、非特許文献１が詳しい。
【特許文献１】特開２００１－２３９１４８号公報
【非特許文献１】ウォーウィック・フォード＋マイケル・バウム著「デジタル署名と暗号技術」　株式会社ピアソン・エデュケーション　１９９７年
【発明の開示】
【発明が解決しようとする課題】
【０００６】
デジタル署名の検証よるメタデータの利用可否判定では、少なくとも１回は不正なメタデータによる障害が発生し、不正発見後にＣＲＬを作成する。このため、万が一にも不正なメタデータによる障害が発生しては困る重要なコンテンツでは、コンテンツプロバイダは、自身がメタデータの中身を確認しデジタル署名したメタデータのみ利用を許可したいという要求がある。この場合、従来のデジタル署名の検証だけでは要求を実現できないという課題がある。

【０００７】
また、ユーザはメタデータを私的に作成しユーザの所有する端末装置のみで利用したいが、従来のデジタル署名によるメタデータの利用可否判定では、全ての端末装置で利用可能にするか利用不可にするかしかできない。このため、ユーザの作成したメタデータの利用範囲をユーザの所有する端末装置だけに限定できないという課題がある。
また、コンテンツプロバイダは、コンテンツによっては、ユーザによるメタデータの作成や編集を制限したい場合や、コンテンツプロバイダが指定したメタデータを利用させたい場合があるが、デジタル署名だけでは実現できないという課題がある。
【０００８】
本発明は、こうした従来の問題点を解決するものであり、コンテンツ配信システムにおいて、コンテンツプロバイダが、コンテンツ毎に、利用可能なメタデータを限定し、ユーザが作成したメタデータの利用範囲を限定することを可能とするメタデータ利用可否判定方法とメタデータ利用可否判定方法による判定を行う端末装置を含むコンテンツ配信システムを提供することを目的としている。
【課題を解決するための手段】
【０００９】
本発明の請求項１記載の情報利用可否判定方法は、第１の情報提供者の提供する第１の情報と、第２の情報提供者から提供される前記第１の情報と関連する第２の情報を利用する端末装置において、第３の情報で指定される情報提供者が署名した前記第２の情報を署名検証し利用可否判定することを特徴としている。
本発明の請求項２記載の情報利用可否判定方法は、請求項１記載の情報利用可否判定方法であって、前記第１の情報が暗号化されている場合に、前記第３の情報が前記第１の情報の暗号鍵を含むライセンスに格納されていることを特徴としている。
【００１０】
本発明の請求項３記載の情報利用可否判定方法は、請求項１記載の情報利用可否判定方法であって、前記第１の情報が暗号化されている場合に、前記第３の情報が暗号化された前記第１の情報に格納されていることを特徴としている。
本発明の請求項４記載の情報利用可否判定方法は、請求項１記載の情報利用可否判定方法であって、前記第２の情報が暗号化されている場合に、前記第３の情報が暗号化された前記第２の情報の暗号鍵を含むライセンスに格納されていることを特徴としている。
【００１１】
本発明の請求項５記載の情報利用可否判定方法は、請求項２～請求項４のいずれか１項に記載の情報利用可否判定方法であって、前記第３の情報が、前記第１の情報提供者のみと、前記第１の情報提供者と前記第１の情報提供者が公開鍵証明書に署名した前記第２の情報提供者のみと、制限なし、のうちの少なくとも２つから１つを識別するフラグであることを特徴としている。
【００１２】
本発明の請求項６記載の情報利用可否判定方法は、請求項２～請求項４のいずれか１項に記載の情報利用可否判定方法であって、前記第３の情報が、前記第２の情報の署名者を一意に特定する識別情報であることを特徴としている。
本発明の請求項７記載の情報利用可否判定方法は、請求項５記載の情報利用可否判定方法であって、前記端末装置に格納されている前記第１の情報提供者の公開鍵証明書を利用することで、前記第１の情報提供者が署名したと判断することを特徴としている。
【００１３】
本発明の請求項８記載の情報利用可否判定方法は、請求項５記載の情報利用可否判定方法であって、前記端末装置に格納されている前記第１の情報提供者を一意に特定する識別情報と前記第２の情報に含まれる署名者を一意に特定する識別情報が一致することで、前記第１の情報提供者が署名したと判断することを特徴としている。
本発明の請求項９記載の情報利用可否判定方法は、請求項５記載の情報利用可否判定方法であって、暗号化されている前記第１の情報に格納されている前記第１の情報提供者を

一意に特定する識別情報と前記第２の情報に含まれる署名者を一意に特定する識別情報が一致することで、前記第１の情報提供者が署名したと判断することを特徴としている。

【００１４】

本発明の請求項１０記載の情報利用可否判定方法は、請求項５記載の情報利用可否判定方法であって、暗号化された前記第２の情報の暗号鍵を含む前記第２の情報のライセンスに含まれている前記第１の情報提供者を一意に特定する識別情報と前記第２の情報に含まれる署名者を一意に特定する識別情報が一致することで、前記第１の情報提供者が署名したと判断することを特徴としている。

【００１５】

本発明の請求項１１記載の情報利用可否判定方法は、請求項２または請求項３記載の情報利用可否判定方法であって、前記端末装置で作成する前記第１の情報と関連する第４の情報に前記端末装置で作成したことを示す識別情報を格納し、前記第４の情報に前記端末装置で作成したことを示す識別情報を含む場合、前記第４の情報の署名検証を行わないことを特徴としている。

【００１６】

本発明の請求項１２記載の情報利用可否判定方法は、請求項１１記載の情報利用可否判定方法であって、前記第４の情報の移動範囲指定情報を含むことを特徴としている。

本発明の請求項１３記載の情報利用可否判定方法は、請求項１１記載の情報利用可否判定方法であって、暗号化された前記第１の情報に前記第４の情報の移動範囲指定情報を含むことを特徴としている。

【００１７】

本発明の請求項１４記載の情報利用可否判定方法は、請求項１１記載の情報利用可否判定方法であって、前記第２の情報のライセンスに前記第４の情報の移動範囲指定情報を含むことを特徴としている。

本発明の請求項１５記載の情報利用可否判定方法は、請求項１１記載の情報利用可否判定方法であって、前記第２の情報に前記第４の情報の移動範囲指定情報を含むことを特徴としている。

【００１８】

本発明の請求項１６記載の情報利用可否判定方法は、請求項１２～請求項１５のいずれか１項に記載の情報利用可否判定方法であって、前記移動範囲指定情報が前記端末装置所有者の所有する前記端末装置に限定する場合に、前記第４の情報の少なくとも一部を前記端末装置所有者の所有する前記端末装置に共通の暗号鍵で暗号化することを特徴としている。

【００１９】

本発明の請求項１７記載の情報利用可否判定方法は、請求項１６記載の情報利用可否判定方法であって、前記第１の情報のライセンスに前記第４の利用可否情報を含むことを特徴としている。

本発明の請求項１８記載の情報利用可否判定方法は、請求項１６記載の情報利用可否判定方法であって、暗号化された前記第１の情報に前記第４の利用可否情報を含むことを特徴としている。

【００２０】

本発明の請求項１９記載の情報利用可否判定方法は、第１の情報提供者の提供する暗号化された第１の情報と、第２の情報提供者から提供される前記第１の情報と関連する第２の情報を利用する端末装置において、前記第１の情報の暗号鍵を含むライセンスに前記第２の情報を用いて前記第１の情報を利用することを指示する参照指示情報を含むことを特徴としている。

【００２１】

本発明の請求項２０記載の情報利用可否判定方法は、第１の情報提供者の提供する暗号化された第１の情報と、第２の情報提供者から提供される前記第１の情報と関連する第２の情報を利用する端末装置において、暗号化された前記第１の情報に前記第２の情報を用

いて前記第１の情報を利用することを指示する参照指示情報を含むことを特徴としている。

【００２２】

本発明の請求項２１記載の情報利用可否判定方法は、請求項１９または請求項２０記載の情報利用可否判定方法であって、前記参照指示情報が前記第２の情報を用いるか否かを識別するフラグであることを特徴としている。

本発明の請求項２２記載の情報利用可否判定方法は、請求項１９または請求項２０記載の情報利用可否判定方法であって、前記参照指示情報が前記第２の情報を一意に特定する識別情報であることを特徴としている。

【００２３】

本発明の請求項２３記載の情報利用可否判定方法は、請求項１９または請求項２０記載の情報利用可否判定方法であって、前記参照指示情報が前記第２の情報の署名者を一意に特定する識別情報であることを特徴としている。

本発明の請求項２４記載の情報利用可否判定方法は、第１の情報提供者の提供する暗号化された第１の情報と、第２の情報提供者から提供される前記第１の情報と関連する第２の情報を利用する端末装置において、前記第１の情報の暗号鍵を含むライセンスに前記第２の情報の編集可否情報を含むことを特徴としている。

【００２４】

本発明の請求項２５記載の情報利用可否判定方法は、第１の情報提供者の提供する暗号化された第１の情報と、第２の情報提供者から提供される前記第１の情報と関連する第２の情報を利用する端末装置において、暗号化された前記第１の情報に前記第２の情報の編集可否情報を含むことを特徴としている。

本発明の請求項２６記載の情報利用可否判定方法は、第１の情報提供者の提供する暗号化された第１の情報と、第２の情報提供者から提供される前記第１の情報と関連する暗号化された第２の情報を利用する端末装置において、暗号化された前記第２の情報の暗号鍵を含むライセンスに前記第２の情報の編集可否情報を含むことを特徴としている。

【００２５】

本発明の請求項２７記載の情報利用可否判定方法は、第１の情報提供者の提供する暗号化された第１の情報と、第２の情報提供者から提供される前記第１の情報と関連する第２の情報を利用する端末装置において、前記第２の情報に前記第２の情報の編集可否情報を含むことを特徴としている。

本発明の請求項２８記載の情報利用可否判定方法は、請求項２４～請求項２７のいずれか１項に記載の情報利用可否判定方法であって、前記編集可否情報が編集可能か否かを識別するフラグであることしている。

【００２６】

本発明の請求項２９記載の情報利用可否判定方法は、請求項２４～請求項２７のいずれか１項に記載の情報利用可否判定方法であって、前記編集可否情報が前記第２の情報を一意に特定する識別方法であることを特徴としている。

本発明の請求項３０記載の情報利用可否判定方法は、請求項２４～請求項２７のいずれか１項に記載の情報利用可否判定方法であって、前記編集可否情報が前記第２の情報の署名者を一意に特定する識別方法であることを特徴としている。

【００２７】

本発明の請求項３１記載のコンテンツ配信システムは、請求項１～請求項３０のいずれか１項に記載の情報利用可否判定方法により、前記第２の情報または前記第４の情報の利用可否を判定する前記端末装置を含むことを特徴としている。

【発明の効果】

【００２８】

本発明によれば、ＣＲＬを用いずに、コンテンツのライセンスにより、利用可能なメタデータをコンテンツプロバイダがデジタル署名したメタデータのみに限定することが可能となる。また、コンテンツプロバイダが指定したメタデータを利用させることが可能とな

る。

さらに、ユーザによるメタデータの作成、および編集を制限することや、ユーザが作成したメタデータの移動範囲を制限することが可能となる。

【発明を実施するための最良の形態】

【００２９】

以下、本発明における実施の形態について、図面を用いて詳細に説明する。

図１は、本発明における実施の形態に関わるコンテンツ配信システム１の全体の概略構成を示す図である。図１に示すように、コンテンツ配信システムは、ライセンス管理サーバ１００と、会員管理サーバ２００と、コンテンツプロバイダ３００と、メタデータプロバイダ４００と、ＣＡ５００と、端末装置６００とを備え、伝送路Ｎで接続されている。

【００３０】

ライセンス管理サーバ１００は、少なくとも、暗号化コンテンツ３１０のライセンス１１０の作成と、ライセンス１１０の端末装置６００への送信を行う。

会員管理サーバ２００は、少なくとも、ユーザ情報ＤＢ２１０を管理し、端末装置６００にドメイン鍵２１２を送信する。

コンテンツプロバイダ３００は、コンテンツ提供者側に設置される装置であって、少なくとも、暗号化コンテンツ３１０の作成と、暗号化コンテンツ３１０の端末装置６００への送信を行う。

【００３１】

メタデータプロバイダ４００は、コンテンツに対するメタデータを作成する作成者側に設定される装置であって、少なくとも、メタデータ４１０の作成と、メタデータ４１０の端末装置６００への送信を行う。

ＣＡ５００は、公開鍵証明書などを作成する作成者側に設置される装置であって、少なくとも、公開鍵証明書５１０の作成と、ＣＲＬ５２０の作成と、ＣＲＬ５２０の端末装置６００への送信を行う。

【００３２】

端末装置６００は、少なくとも、暗号化コンテンツ３１０と、メタデータ４１０の利用を行う。尚、端末装置６００には耐タンパ部があり、認証通信や暗号鍵の取得や暗号化や復号などの暗号が関連する処理は、暗号鍵の流出などが発生しないように耐タンパ部で行われる。

伝送路Ｎは、インターネット等の通信ネットワークや、デジタル放送、あるいは、これらが複合したネットワークである。

【００３３】

次に、コンテンツ配信システム１の各構成要素が保有するデータについて説明する。

（１）ライセンス１１０

ライセンス管理サーバ１００は、図２に示すライセンス１１０を保有し、端末装置６００に送信する。ライセンス１１０は、ライセンスＩＤ１１１と、コンテンツＩＤ１１２と、コンテンツプロバイダＩＤ１１３と、利用条件１１４と、コンテンツ暗号鍵１１５から構成されている。

【００３４】

ライセンスＩＤ１１１は、ライセンス管理サーバ１００でのライセンス１１０の識別に用いる。コンテンツＩＤ１１２は、ライセンス１１０と暗号化コンテンツ３１０を対応付けるために用いる。コンテンツプロバイダＩＤ１１３は、ライセンス１１０で制御されるコンテンツのコンテンツプロバイダの識別に用いる。利用条件１１４は、コンテンツの利用制御に用いる。利用条件１１４は、例えば、“３回利用可能”などの情報である。コンテンツ暗号鍵１１５はコンテンツの復号に用いる。

【００３５】

（２）ユーザ情報ＤＢ２１０

会員管理サーバ２００は、図３に示すユーザ情報ＤＢ２１０を保有し、端末装置６００からの端末登録要求に応じて、ドメイン鍵２１２を送信する。ユーザ情報ＤＢ２１０は、

ユーザＩＤ２１１と、ドメイン鍵２１２の組から構成される。
ユーザＩＤ２１１とは、端末装置６００の所有者毎に与えられるＩＤである。
【００３６】
ドメインとはユーザの所有する端末装置６００で構成される集合であり、ドメイン鍵２１２とは、同じドメイン鍵２１２を持つ端末装置間のみにデータの送受信が限定されるように、データの暗号化や、認証通信に用いる暗号鍵のことである。
例えば、図３において、「ＸＸＸＡＡＡ」のユーザＩＤ２１１に対して、「ＸＸＸＣＣＣ」のドメイン鍵２１２が割り当てられていることを示している。
【００３７】
（３）暗号化コンテンツ３１０
コンテンツプロバイダ（ＣＰ）３００は、コンテンツプロバイダＩＤ１１３と、コンテンツプロバイダの秘密鍵と、当該秘密鍵に対する公開鍵と、公開鍵証明書と、コンテンツ暗号鍵１１５と、図４に示す暗号化コンテンツ３１０を保有する。
暗号化コンテンツ３１０はコンテンツＩＤ３１１と、コンテンツプロバイダＩＤ３１２と、コンテンツ本体３１３から構成され、ライセンス１１０のコンテンツ暗号鍵１１５でコンテンツプロバイダＩＤ３１２とコンテンツ本体３１３が暗号化されている。
【００３８】
コンテンツＩＤ３１１は、ライセンス１１０と暗号化コンテンツ３１０を対応付けるために用いる。コンテンツプロバイダＩＤ３１２は、暗号化コンテンツ３１０の提供者を識別するために用いる。コンテンツ本体３１３は、映像または音楽などのデジタルデータである。
【００３９】
（４）メタデータ４１０
メタデータプロバイダ４００は、メタデータプロバイダＩＤと、メタデータプロバイダの秘密鍵と、当該秘密鍵に対する公開鍵と、公開鍵証明書５１０と、図５に示すメタデータ４１０を保有する。
【００４０】
メタデータ４１０は、メタデータ本体４１１と、メタデータ署名者ＩＤ４１２と、デジタル署名４１３とから構成されている。メタデータ本体４１１にはメタデータを識別するためのメタデータＩＤと、コンテンツＩＤなどの属性情報と、コンテンツの位置情報と、シーンインデックスなどのコンテンツの制御情報などが含まれる。メタデータ署名者ＩＤ４１２は、メタデータ４１０にデジタル署名した署名者を識別するために用いる。デジタル署名４１３は、メタデータ本体４１１の改ざん検出に用いる。
【００４１】
（５）ＣＲＬ５２０
ＣＡ（Ｃｅｒｔｉｆｉｃａｔｉｏｎ　Ａｕｔｈｏｒｉｔｙ）５００は、図７に示すＣＲＬ５２０と、ＣＡの秘密鍵と、公開鍵を保有する。
ＣＲＬ５２０は、少なくとも、更新日時５２１とリボークされた主体者ＩＤ５２２から構成されている。リボークとは、主体者ＩＤ５２２で特定される署名者によるデジタル署名を無効化することである。更新日時５２１は、例えば、ＣＲＬ５２０を作成した日付であり、ＣＲＬ５２０のバージョン確認に用いる。リボークされた主体者ＩＤ５２２は、無効化する署名者の識別に用いる。
【００４２】
（６）公開鍵証明書５１０
また、コンテンツプロバイダ３００およびメタデータプロバイダ４００が主体者として図６に示す公開鍵証明書５１０の作成を依頼した時、主体者公開鍵５１２と引き換えに公開鍵証明書５１０を主体者に送信する。
公開鍵証明書５１０は、少なくとも、主体者ＩＤ５１１と、主体者公開鍵５１２と、デジタル署名５１３と、証明書署名者ＩＤ５１４から構成されている。
【００４３】

尚、主体者ＩＤ５１１は公開鍵証明書５１０の主体者を識別するＩＤであり、例えば、Ｘ．５０９の証明書におけるシリアル番号を用いてもよい。主体者公開鍵５１２は、主体者ＩＤ５１１で特定される署名者のデジタル署名の検証に用いる。デジタル署名５１３は、少なくとも、主体者ＩＤ５１１と、主体者公開鍵５１２の改ざん検出に用いる。証明書署名者ＩＤ５１４は、公開鍵証明書５１０にデジタル署名した署名者の特定に用いる。

【００４４】

コンテンツ配信システム１におけるメタデータ４１０とコンテンツ利用処理概略は、例えば、図１０に示す手順で行われる。

以降にコンテンツ配信システム１の各構成要素の処理について説明する。

端末装置６００は、会員管理サーバ２００からドメイン鍵２１２を取得（ステップＳ１０００）し、コンテンツプロバイダ３００から暗号化コンテンツ３１０を受信（ステップＳ１０１０）し、ライセンス管理サーバ１００からライセンス１１０を受信（ステップＳ１０２０）し、メタデータプロバイダ４００からメタデータ４１０を受信（ステップＳ１０３０）し、メタデータ４１０とコンテンツを利用（ステップＳ１０４０）する。

【００４５】

会員管理サーバ２００は、端末装置６００にドメイン鍵２１２を配信（ステップＳ１１００）する。

コンテンツプロバイダ３００は、暗号化コンテンツ３１０を作成（ステップＳ１２００）し、端末装置６００に暗号化コンテンツ３１０を送信（ステップＳ１２１０）する。

ライセンス管理サーバ１００は、ライセンス１１０を作成（ステップＳ１３００）し、端末装置６００にライセンス１１０を送信（ステップＳ１３１０）する。

【００４６】

メタデータプロバイダ４００は、メタデータ４１０を作成（ステップＳ１４００）し、端末装置６００にメタデータ４１０を送信（ステップＳ１４１０）する。

図示しないが、ＣＡ５００は、コンテンツプロバイダ３００と、メタデータプロバイダ４００から公開鍵証明書５１０の要求がある都度、公開鍵証明書５１０を作成して、要求したコンテンツプロバイダ３００と、メタデータプロバイダ４００に送信し、コンテンツプロバイダ３００からメタデータプロバイダ４００のリボーク要求がある都度、ＣＲＬを作成して端末装置６００に送信する。

【００４７】

尚、以下の説明に記述されるコンテンツの暗号化方式は、ＡＥＳ（Ａｄｖａｎｃｅｄ Ｅｎｃｒｙｐｔｉｏｎ Ｓｔａｎｄａｒｄ）やＴｒｉｐｌｅ ＤＥＳ（Ｄａｔａ Ｅｎｃｒｙｐｔｉｏｎ Ｓｔａｎｄａｒｄ）等の共通鍵暗号アルゴリズムが、デジタル署名の方式には、ＲＳＡやＥＣ－ＤＳＡ（Ｅｌｌｉｐｔｉｃ Ｃｕｒｖｅ Ｄｉｇｉｔａｌ Ｓｉｇｎａｔｕｒｅ Ａｌｇｏｒｉｔｈｍ）等の公開鍵暗号アルゴリズムが用いられるのが一般的であり、以下に説明する処理は特定の暗号方式に依存しない。また、ハッシュ計算方式は、ＳＨＡ－１（Ｓｅｃｕｒｅ Ｈａｓｈ Ａｌｇｏｒｉｔｈｍ １）やＭＤ５等が用いられるのが一般的であり、以下に説明する処理は特定のハッシュ計算方式に依存しない。

【００４８】

また、ライセンス管理サーバ１００と、会員管理サーバ２００と、コンテンツプロバイダ３００とメタデータプロバイダ４００とから端末装置６００に送信されるコンテンツ選択画面等のユーザインタフェース画面は、インターネットを通じて、ＨＴＴＰ等のプロトコルにより送信される、ＨＴＭＬ（ＨｙｐｅｒＴｅｘｔ Ｍａｒｋｕｐ Ｌａｎｇｕａｇｅ）やＸＭＬ（Ｅｘｔｅｎｓｉｂｌｅ Ｍａｒｋｕｐ Ｌａｎｇｕａｇｅ）等のスクリプト言語で記述されたウェブページ、あるいは、デジタル放送により送信される、ＢＭＬ（Ｂｒｏａｄｃａｓｔｉｎｇ Ｍａｒｋｕｐ Ｌａｎｇｕａｇｅ）で記述されたページが一般的であり、以下に説明する処理は特定のページ記述方式に依存しない。

【００４９】

会員管理サーバ２００の処理について説明する。

（ドメイン鍵送信Ｓ１１００）

会員管理サーバ２００は、端末装置６００からのユーザＩＤ２１１を含む端末登録要求を受信し、ユーザ情報ＤＢ２１０から対応するドメイン鍵２１２を取得し送信する。尚、ユーザ情報ＤＢ２１０にはユーザＩＤ２１１とドメイン鍵２１２があらかじめ登録されている。

コンテンツプロバイダ３００の処理について説明する。

【００５０】

（暗号化コンテンツ作成Ｓ１２００）

コンテンツプロバイダ３００は、コンテンツ本体３１３に対して、コンテンツ毎に異なるコンテンツＩＤ３１１と、コンテンツプロバイダ毎に異なるコンテンツプロバイダＩＤ３１２をつけて、コンテンツプロバイダＩＤ３１２とコンテンツ本体３１３をコンテンツ暗号鍵１１５で暗号化して暗号化コンテンツ３１０を作成する。

【００５１】

（暗号化コンテンツ送信Ｓ１２１０）

コンテンツプロバイダ３００は、端末装置６００のコンテンツ選択要求に応じて、コンテンツ選択画面を作成し、端末装置６００へ送信する。コンテンツ選択画面は端末装置６００がコンテンツを選択すると対応するコンテンツＩＤ３１１を含むコンテンツ取得要求がコンテンツプロバイダ３００に送信されるようになっており、コンテンツプロバイダ３００はコンテンツ取得要求に含まれるコンテンツＩＤ３１１に対応した暗号化コンテンツ３１０を端末装置６００に送信する。尚、コンテンツプロバイダ３００から端末装置６００への暗号化コンテンツ３１０の送信は、ストリーミングでもファイル配信でもよい。

ライセンス管理サーバ１００の処理について説明する。

【００５２】

（ライセンス作成Ｓ１３００）

ライセンス管理サーバ１００は、コンテンツプロバイダ３００からコンテンツＩＤ１１２とコンテンツプロバイダＩＤ１１３と利用条件１１４とコンテンツ暗号鍵１１５を受信し、ライセンスＩＤ１１１をつけてライセンス１１０を作成する。利用条件１１４には、コンテンツの利用制御とメタデータ４１０の利用制御に関する情報が含まれている。

【００５３】

コンテンツの利用制御に関する情報としては、利用有効期限情報と、利用可能回数情報などがある。

利用有効期限情報としては、例えば、“２００５年１２月３１日まで利用可能”などの情報が含まれる。

利用可能回数情報としては、例えば、“３回利用可能”などの情報が含まれる。

【００５４】

メタデータの利用制御に関する情報としては、メタデータの署名者識別情報と、メタデータの参照指示情報と、メタデータの編集可否情報と、ユーザ作成メタデータによる制御可否情報と、ユーザ作成メタデータの移動範囲指定情報などがある。

メタデータの署名者識別情報としては、例えば、メタデータの署名者として、“コンテンツプロバイダ以外不可”または“コンテンツプロバイダおよびコンテンツプロバイダに委任されたメタデータプロバイダ可能”または“全て可能””などの署名者識別情報が含まれる。ここで、コンテンツプロバイダに委任されたメタデータプロバイダとは、コンテンツプロバイダ３００がデジタル署名した公開鍵証明書５１０を持つメタデータプロバイダ４００のことであり、それ以外のメタデータプロバイダ４００よりもコンテンツプロバイダ３００にとっての信頼性は高い。

【００５５】

尚、メタデータの署名者識別情報は、利用を許可または不許可するメタデータ署名者ＩＤ４１２でもよい。

メタデータの参照指示情報としては、例えば、暗号化コンテンツ３１０とともに配信するメタデータ４１０の参照を強制したい場合には、メタデータ参照指示フラグが含まれる

。尚、参照指示情報はメタデータ参照指示フラグ、あるいは、参照を強制させたいメタデータのＩＤ、あるいは、メタデータの署名者ＩＤのいずれでもよい。尚、本実施の形態では、コンテンツのライセンスにメタデータの参照指示情報を含む例について記述するが、暗号化コンテンツ３１０に参照指示情報を含む場合でもよい。

【００５６】

メタデータの編集可否情報としては、例えば、“メタデータ編集可能”または“メタデータ編集不可”を示すフラグ、あるいは、編集可能なまたは編集不可能なメタデータのＩＤ、あるいは、編集可能なまたは編集不可能なメタデータデジタル署名のメタデータ署名者ＩＤ４１２のいずれでもよい。尚、本実施の形態では、メタデータの編集可否情報がコンテンツのライセンスに含まれる場合について記述するが、暗号化コンテンツ３１０に含まれる場合、あるいは、メタデータ４１０のメタデータ本体４１１に含まれる場合、あるいは、コンテンツと同様にメタデータ４１０が暗号化され、暗号鍵を含むメタデータ４１０のライセンスがある場合、メタデータ４１０のライセンスに含まれる場合のいずれでもよい。

【００５７】

ユーザ作成メタデータによる制御可否情報としては、例えば、“ユーザ作成メタデータによる制御可能”または“ユーザ作成メタデータによる制御不可”を示すフラグなどの情報が含まれる。尚、本実施の形態では、ユーザ作成メタデータによる制御可否情報がコンテンツのライセンスに含まれる場合について記述するが、暗号化コンテンツ３１０に含まれる場合でもよい。

【００５８】

ユーザ作成メタデータの移動範囲指定情報としては、例えば、“移動無制限”または“メタデータを作成したユーザが所有する端末装置に限定”などの移動可能範囲を示す情報が含まれる。尚、本実施の形態では、ユーザ作成メタデータの移動範囲指定情報がコンテンツのライセンスに含まれる場合について記述するが、暗号化コンテンツ３１０に含まれる場合、あるいは、メタデータ４１０のメタデータ本体４１１に含まれる場合、あるいは、コンテンツと同様にメタデータが暗号化され、暗号鍵を含むメタデータのライセンスがある場合、メタデータのライセンスに含まれる場合のいずれでもよい。

【００５９】

（ライセンス送信Ｓ１３１０）

ライセンス管理サーバ１００は、端末装置６００からのライセンス取得要求に応じてライセンスの購入処理を行った後、端末装置６００にライセンス１１０を送信する。尚、ライセンスの購入処理は図示しない購入サーバとライセンス管理サーバ１００との間で行われる。

【００６０】

メタデータプロバイダ４００の処理について説明する。

（メタデータ作成Ｓ１４００）

メタデータプロバイダ４００は、メタデータ本体４１１を作成し、署名者４１２にメタデータプロバイダのＩＤを格納し、メタデータ本体４１１とメタデータ署名者ＩＤ４１２に対するデジタル署名４１３を作成する。メタデータ４１０のデジタル署名をコンテンツプロバイダ３００が行う場合もあり、その場合には、メタデータプロバイダ４００からコンテンツプロバイダ３００にメタデータ本体４１１を送信し、コンテンツプロバイダ３００が、メタデータ署名者ＩＤ４１２にコンテンツプロバイダのＩＤを格納し、コンテンツプロバイダのデジタル署名４１３を作成してメタデータ４１０を作成し、メタデータプロバイダ４００に送信する。

【００６１】

（メタデータ送信Ｓ１４１０）

メタデータプロバイダ４００は、端末装置６００からのメタデータ取得要求に応じて、メタデータ選択画面を作成し、端末装置６００送信する。メタデータ選択画面は端末装置６００がメタデータを選択すると対応するメタデータＩＤを含むメタデータ取得要求がメ

タデータプロバイダ４００に送信されるようになっており、メタデータプロバイダ４００はメタデータ取得要求に含まれるメタデータＩＤに対応したメタデータ４１０を端末装置６００に送信する。

ＣＡ５００の処理について説明する。

【００６２】

（公開鍵証明書作成）

ＣＡ５００は、コンテンツプロバイダ３００またはメタデータプロバイダ４００から主体者公開鍵５１２を含む公開鍵証明書５１０の作成要求を受信し、主体者公開鍵５１２毎に異なる主体者ＩＤ５１１を生成し、主体者ＩＤ５１１と主体者公開鍵５１２に対するデジタル署名５１３を作成し、主体者ＩＤ５１１と、主体者公開鍵５１２と、デジタル署名５１３とから構成される公開鍵証明書５１０を作成しコンテンツプロバイダ３００またはメタデータプロバイダ４００に送信する。

【００６３】

尚、コンテンツプロバイダ３００が、信頼するメタデータプロバイダ４００にメタデータのデジタル署名を委任する場合などに、コンテンツプロバイダ３００が、メタデータプロバイダ４００の公開鍵証明書５１０の作成処理を行うことがある。この場合、コンテンツプロバイダ３００がデジタル署名した公開鍵証明書５１０を持つメタデータプロバイダ４００は、それ以外のメタデータプロバイダ４００よりもコンテンツプロバイダ３００に信頼されていると判断する場合もある。このような方法は、証明書パスと呼ばれる一般的な方法で、非特許文献１が詳しい。

【００６４】

（ＣＲＬ作成）

ＣＡ５００は、コンテンツプロバイダ３００からリボーク対象のメタデータプロバイダ４００のＩＤを含むＣＲＬ更新要求を受信し、更新日時５２１を、例えば、“２００３年１月１日”から“２００３年１１月１１日”のように、ＣＲＬ作成日時に更新し、受信したメタデータプロバイダ４００のＩＤを主体者ＩＤ５２２に追加し、ＣＲＬ５２０を作成し端末装置６００に送信する。

端末装置６００の処置について説明する。

【００６５】

（ドメイン鍵受信Ｓ１０００）

まず、端末装置６００のドメイン鍵受信処理について説明する。

端末装置６００は、会員管理サーバ２００に会員登録要求を送信し、ドメイン鍵２１２を受信する。ドメイン鍵２１２は端末装置６００に格納される。通信路Ｎを通じて、会員管理サーバ２００と端末装置６００との間でドメイン鍵２１２を送受信する場合には、セキュリティを確保するため、ＳＳＬ（Ｓｅｃｕｒｅ　Ｓｏｃｋｅｔ　Ｌａｙｅｒ）などの安全な認証チャネル（Ｓｅｃｕｒｅ　Ａｕｔｈｅｎｔｉｃａｔｅｄ　Ｃｈａｎｎｅｌ、以下、ＳＡＣと記述）を確立してから、データの送受信を行う。端末装置６００は、受信したライセンス１１０を端末装置６００に格納する。尚、本実施の形態では、会員管理サーバ２００と端末装置６００との間でＳＡＣを確立してからドメイン鍵２１２を送受信したが、端末装置６００に固有鍵が格納されており、会員管理サーバ２００が各端末装置６００の固有鍵を管理している場合には、ドメイン鍵２１２を端末装置６００の固有鍵で暗号化して会員管理サーバ２００から端末装置６００に送信するなどしてもよい。

【００６６】

（暗号化コンテンツ受信Ｓ１０１０）

次に、暗号化コンテンツ３１０の受信処理について説明する。

端末装置６００は、コンテンツプロバイダ３００に、コンテンツ選択要求を送信し、コンテンツ選択画面を受信する。端末装置６００は受信したコンテンツ選択画面を表示し、ユーザの操作により選択されたコンテンツのコンテンツＩＤ３１１を含むコンテンツ取得要求をコンテンツプロバイダ３００に送信し、コンテンツプロバイダ３００から暗号化コンテンツ３１０を受信する。尚、コンテンツプロバイダ３００から端末装置６００への暗

号化コンテンツ３１０の送信は、ストリーミングでもファイル配信でもよい。

【００６７】

（ライセンス受信Ｓ１０２０）

次に、コンテンツのライセンス１１０の受信処理について説明する。

端末装置６００は、ライセンス管理サーバ１００に、ライセンス選択要求を送信し、ライセンス選択画面を受信する。端末装置６００は受信したライセンス選択画面を表示し、端末装置６００は、ユーザの操作により選択されたライセンス１１０のライセンス１１１ＩＤを含むライセンス購入要求をライセンス管理サーバ１００に送信し、ライセンス管理サーバ１００からライセンス１１０を受信する。通信路Ｎを通じて、ライセンス管理サーバ１００と端末装置６００との間でライセンス１１０を送受信する場合には、セキュリティを確保するため、ＳＡＣを確立してから、データの送受信を行う。端末装置６００は、受信したライセンス１１０を端末装置６００に格納する。尚、本実施の形態では、ライセンス管理サーバ１００と端末装置６００との間でＳＡＣを確立してからライセンス１１０を送受信するが、端末装置６００に固有鍵が格納されており、ライセンス管理サーバ１００が各端末装置６００の固有鍵を管理している場合には、ライセンス１１０を端末装置６００の固有鍵で暗号化してライセンス管理サーバ１００から端末装置６００に送信するなどしてもよい。

【００６８】

（メタデータ受信Ｓ１０２０）

次に、メタデータ４１０の受信処理について説明する。

端末装置６００は、メタデータプロバイダ４００に、メタデータ選択要求を送信し、メタデータ選択画面を受信する。端末装置６００は受信したメタデータ選択画面を表示し、ユーザの操作により選択されたメタデータ４１０のメタデータＩＤを含むメタデータ取得要求をメタデータプロバイダ４００に送信し、メタデータプロバイダ４００からメタデータ４１０を受信する。

【００６９】

（公開鍵証明書受信）

次に、公開鍵証明書５１０の受信処理について説明する。

端末装置６００は、コンテンツプロバイダ３００に、公開鍵証明書要求を送信し、コンテンツプロバイダ３００の公開鍵証明書５１０を受信する。

端末装置６００は、メタデータプロバイダ４００に、公開鍵証明書要求を送信し、メタデータプロバイダ４００の公開鍵証明書５１０を受信する。

端末装置６００は、ＣＡ５００に、公開鍵証明書要求を送信し、ＣＡ５００の公開鍵証明書５１０を受信する。

【００７０】

（メタデータとコンテンツ利用Ｓ１０４０）

次にコンテンツプロバイダ３００またはメタデータプロバイダ４００が署名したメタデータの利用可否判定について図８を用いて説明する。

メタデータ４１０がユーザ作成メタデータであるか否か判定する（ステップＳ２００）。ユーザ作成メタデータ判定（ステップＳ２００）の処理については後述する。ユーザ作成メタデータでない場合は署名者識別情報判定（ステップＳ１００）に遷移し、ユーザ作成メタデータの場合（後述する値「０」の場合）はステップＳ２０１に遷移する。

署名者識別情報判定（ステップＳ１００）では、ライセンス１１０の利用条件１１４から署名者識別情報を取得し、“コンテンツプロバイダ以外不可”または“コンテンツプロバイダおよびコンテンツプロバイダに委任されたメタデータプロバイダ可能”または“全て可能”のいずれであるか判定する。

【００７１】

署名者識別情報が“コンテンツプロバイダ以外不可”または“コンテンツプロバイダおよびコンテンツプロバイダに委任されたメタデータプロバイダ可能”の場合には、ＩＤ比較（ステップＳ１０１）に遷移する。

署名者識別情報が“全て可能”の場合にはＣＲＬ確認（ステップＳ１１０）に遷移する。

【００７２】

ＩＤ比較（ステップＳ１０１）について図１１を用いて説明する。

ＩＤ比較（ステップＳ１０１）では、暗号化コンテンツ３１０をコンテンツ暗号鍵１１５で復号してコンテンツプロバイダＩＤ３１２を取得し、メタデータ４１０からメタデータ署名者ＩＤ４１２を取得し、比較する（ステップＳ３０１）。コンテンツプロバイダＩＤ３１２とメタデータ署名者ＩＤ４１２が一致する場合は署名検証（ステップＳ１０２）に遷移する。コンテンツプロバイダＩＤ３１２とメタデータ署名者ＩＤ４１２が一致しない場合は、署名者識別情報を確認する（ステップＳ３０２）。

【００７３】

署名者識別情報が“コンテンツプロバイダ以外不可”の場合は、署名者識別情報で利用可能なメタデータの署名者が“コンテンツプロバイダ以外不可“と設定されているのに、メタデータ４１０の署名者がコンテンツプロバイダ３００以外であるため、メタデータ４１０は利用不可である。

署名者識別情報が“コンテンツプロバイダおよびコンテンツプロバイダに委任されたメタデータプロバイダ可能”の場合は、メタデータ署名者ＩＤ４１２と主体者ＩＤ５１１が一致する公開鍵証明書５１０の証明書署名者ＩＤ５１４とコンテンツプロバイダＩＤ３１２とを比較する（ステップＳ３０３）。証明書署名者ＩＤ５１４とコンテンツプロバイダＩＤ３１２とが一致する場合は、署名検証（ステップ１０２）に遷移する。証明書署名者ＩＤ５１４とコンテンツプロバイダＩＤ３１２が一致しない場合は、署名者識別情報で利用可能なメタデータの署名者が“コンテンツプロバイダおよびコンテンツプロバイダに委任されたメタデータプロバイダ可能“と設定されているのに、メタデータの署名者がコンテンツプロバイダ３００およびコンテンツプロバイダ３００に委任されたメタデータプロバイダ４００以外であるため、メタデータ４１０は利用不可である。

【００７４】

署名検証（ステップＳ１０２）では、メタデータのデジタル署名のメタデータ署名者ＩＤ４１２と一致する主体者ＩＤ５１１を含む公開鍵証明書５１０を取得し、公開鍵証明書５１０に含まれる主体者公開鍵５１２を用いてメタデータのデジタル署名を復号し、メタデータ本体４１１とメタデータ署名者ＩＤ４１２のハッシュ値と比較し、一致する場合はメタデータ４１０が利用可能と判定し、一致しない場合は改ざんされているために利用不可と判定する。

【００７５】

ＣＲＬ確認（ステップＳ１１０）では、メタデータ４１０のメタデータ署名者ＩＤ４１２がＣＲＬ５２０のリボークされた主体者ＩＤ５２２に含まれているか判定し、含まれていない場合には、署名検証（ステップＳ１０２）に遷移し、含まれている場合には、署名者がリボークされているためにメタデータ４１０は利用不可と判定する。

以上の処理により、ライセンス１１０の利用条件１１４に格納されている署名者識別情報に基づきメタデータの利用可否を判定することが可能となる。

【００７６】

尚、本実施の形態では、署名者識別情報を“コンテンツプロバイダ以外不可”または“コンテンツプロバイダおよびコンテンツプロバイダに委任されたメタデータプロバイダ可能”または“全て可能”の３つの値から１つの値を識別するフラグとしたが、“コンテンツプロバイダ以外不可”または“コンテンツプロバイダおよびコンテンツプロバイダに委任されたメタデータプロバイダ可能”または“全て可能”のうちの少なくとも２つの値から１つの値を識別するフラグとしてもよい。この場合、例えば、署名者識別情報が“コンテンツプロバイダ以外不可”または “全て可能”を識別するフラグであれば、本実施の形態における署名者識別情報が“コンテンツプロバイダおよびコンテンツプロバイダに委任されたメタデータプロバイダ可能”である場合の処理が行われなくなり、署名者識別情報が“コンテンツプロバイダ以外不可”または “コンテンツプロバイダおよびコンテン

ツプロバイダに委任されたメタデータプロバイダ可能”を識別するフラグであれば、本実施の形態における署名者識別情報が“全て可能”である場合の処理が行われなくなるが同様の効果をもたらす。

【００７７】

尚、本実施の形態では、署名者識別情報判定（ステップＳ１００）で署名者識別情報が、“コンテンツプロバイダ以外不可”または“コンテンツプロバイダおよびコンテンツプロバイダに委任されたメタデータプロバイダ可能”の場合にＣＲＬ確認（ステップＳ１１０）を行わないが、署名者識別情報判定（ステップＳ１００）以降に行ってもよい。

尚、本実施の形態では、コンテンツライセンス１１０の利用条件１１４に署名者識別情報が格納されているが、コンテンツライセンス１１０の中の利用条件１１４以外に格納されていてもよい。また、署名者識別情報が暗号化コンテンツ３１０に格納されていてもよい。また、コンテンツと同様にメタデータが暗号化され、暗号鍵を含むメタデータ４１０のライセンスがある場合、署名者識別情報がメタデータ４１０のライセンスに格納されていてもよい。以上の場合、署名者識別情報の取得先が異なるが同様の効果をもたらす。

尚、本実施の形態では、署名者識別情報を“コンテンツプロバイダ以外不可”または“コンテンツプロバイダおよびコンテンツプロバイダに委任されたメタデータプロバイダ可能”または“全て可能”を示すフラグとしたが、メタデータ４１０のメタデータ署名者ＩＤ４１２としてもよい。この場合、利用可能なメタデータの署名者がメタデータ署名者ＩＤ４１２の署名者に限定されるが同様の効果をもたらす。

【００７８】

尚、本実施の形態では、メタデータ４１０のメタデータ署名者ＩＤ４１２がコンテンツプロバイダＩＤであるか否かのＩＤ比較（ステップＳ１０１）に、暗号化コンテンツ３１０に含まれているコンテンツプロバイダＩＤ３１２を用いているが、端末装置６００に出荷時などあらかじめコンテンツプロバイダの公開鍵証明書５１０のみが格納されている場合には、公開鍵証明書５１０に含まれている主体者ＩＤ５１１を用いてもよい。また、端末装置６００に出荷時などにあらかじめコンテンツプロバイダＩＤのみが格納されている場合には、格納されているコンテンツプロバイダＩＤを用いてもよい。また、メタデータ４１０のライセンスがあり、メタデータ４１０のライセンスにコンテンツプロバイダＩＤが格納されている場合、メタデータ４１０のライセンスのコンテンツプロバイダＩＤを用いてもよい。以上のいずれの場合でも、コンテンツプロバイダ３００のコンテンツプロバイダＩＤが特定できるため同様の効果をもたらす。

【００７９】

次に、ユーザによるメタデータの作成処理について説明する。

ユーザの入力操作に従い、端末装置６００は、メタデータを作成する。具体的には、ユーザ作成メタデータであることを示すユーザ作成フラグと、シーンインデックスなどの情報とをメタデータ本体４１１に格納し、メタデータ作成者がユーザであることを示すために、メタデータ署名者ＩＤ４１２に値０を格納し、デジタル署名４１３にデジタル署名せずに値０を格納する。

【００８０】

尚、本実施の形態では、メタデータ署名者ＩＤ４１２とデジタル署名４１３に値０を格納する場合について記述するが、ユーザにより端末装置６００で作成されたメタデータ４１０を識別できれば他の値でもよい。

尚、本実施の形態では、ユーザ作成メタデータにデジタル署名しないが、全端末装置６００がメタデータ署名者ＩＤ４１２と、秘密鍵と、公開鍵証明書５１０を保有している場合には、デジタル署名してもよい。この場合、後述するユーザ作成メタ判定（ステップＳ２００）では、メタデータ４１０のデジタル署名者がユーザの所有する端末装置６００であるか否かの判定を行う。

【００８１】

端末装置６００は、ライセンス１１０の利用条件１１４からユーザ作成メタデータの移

動範囲指定情報を取得し、“移動無制限”であれば、上記処理で作成したメタデータをそのまま端末装置６００などに蓄積し、“メタデータを作成したユーザが所有する端末装置に限定”であれば、メタデータ本体４１１をドメイン鍵２１２で暗号化して端末装置６００やＤＶＤ－Ｒなどの外部記憶媒体などに蓄積するか、ユーザが所有する他の端末装置６００に送信する。この場合、メタデータ本体４１１がドメイン鍵で暗号化されているため、異なるドメインの端末装置６００がメタデータ４１０を取得しても利用できない。

【００８２】

尚、本実施の形態では、ユーザ作成メタデータの移動範囲指定情報が“メタデータを作成したユーザが所有する端末装置に限定”の場合にドメイン鍵２１２を用いてメタデータ本体２１２を暗号化しているが、ユーザが所有する端末装置６００に共通の秘密情報であれば他の情報を用いてもよい。

【００８３】

次にユーザが作成したメタデータの利用可否判定について図９を用いて説明する。

端末装置６００は、ユーザ作成メタ判定（ステップＳ２００）を行う。

ユーザ作成メタ判定（ステップＳ２００）では、メタデータ４１０のメタデータ署名者ＩＤ４１２が値０であるか判定する。値０でない場合は署名者識別情報判定（ステップＳ１００）に遷移し、値０の場合はユーザ作成メタ利用可否判定（ステップＳ２０１）に遷移する。

【００８４】

ユーザ作成メタ利用可否判定（ステップＳ２０１）では、ライセンス１１０の利用条件１１４からユーザ作成メタデータによる制御可否情報を取得し、“ユーザ作成メタデータによる制御不可”であれば、メタデータ４１０は利用不可である。ユーザ作成メタデータによる制御可否情報が“ユーザ作成メタデータによる制御可能”の場合には、ユーザ作成メタデータ移動範囲判定（ステップＳ２０２）に遷移する。

【００８５】

ユーザ作成メタデータ移動範囲判定（ステップＳ２０２）では、ライセンス１１０の利用条件１１４からユーザ作成メタデータの移動範囲指定情報を取得し、“移動無制限”であれば、上記処理で作成したメタデータ４１０は利用可能と判定する。ユーザ作成メタデータの移動範囲指定情報が“メタデータを作成したユーザが所有する端末装置に限定”であれば、メタデータ本体４１１をドメイン鍵２１２で復号し、ユーザ作成メタデータであることを示すユーザ作成フラグがあるか否か判定する（ステップＳ２０３）。ユーザ作成フラグがない場合には、メタデータ４１０は利用不可である。ユーザ作成フラグがある場合には、メタデータ４１０は利用可能と判定する。

【００８６】

尚、本実施の形態では、移動範囲指定情報を、“ユーザ作成メタデータによる制御可能”または“ユーザ作成メタデータによる制御不可”のいずれかを示すフラグとし、移動範囲指定情報が“ユーザ作成メタデータによる制御可能”の場合には、ドメイン鍵２１２を用いてユーザ作成メタデータを暗号化することで、ユーザ作成メタデータの移動範囲をユーザの所有する端末装置６００間に限定しているが、移動範囲指定情報として移動回数や移動有効期間などの利用条件を格納し、端末装置６００で生成した暗号鍵でユーザ作成メタデータを暗号化し、暗号鍵を含むユーザ作成メタデータのライセンスに移動範囲指定情報として格納された移動回数や移動有効期間などの利用条件を設定することで、移動を制限することにしてもよい。この場合、ユーザ作成メタデータの移動範囲は、移動範囲指定情報として格納された移動回数や移動有効期間などにより制限される。

【００８７】

以降に、上記の判定処理でメタデータ４１０が利用可能と判定した後で行う処理について説明する。

まず、メタデータ参照必須コンテンツの利用処理について説明する。

端末装置６００は、ライセンス１１０の利用条件１１４からメタデータの参照指示情報があるか否か検索し、参照指示情報がない場合は、暗号化コンテンツ３１０の利用を開始

する。参照指示情報がある場合は参照指示情報を取得し、参照指示情報に含まれるメタデータＩＤから参照すべきメタデータを取得し、メタデータの利用可否判定で利用可能な場合にメタデータを参照してコンテンツの利用を開始する。参照すべきメタデータが取得できない場合と、メタデータの利用可否判定で利用不可の場合にはコンテンツの利用ができない。

【００８８】

尚、本実施の形態では、参照指示情報をメタデータＩＤとしたが、メタデータ署名者ＩＤ４１２でもよい。

尚、本実施の形態では、参照指示情報をメタデータＩＤとしたが、例えば、暗号化コンテンツ３１０とメタデータ４１０が共に端末装置６００に送信されるなどして、暗号化コンテンツ３１０とメタデータ４１０が関連付けられている場合には、参照指示情報は、参照するか参照しないかを識別するフラグでもよい。

【００８９】

次にユーザによるメタデータの編集処理について説明する。

端末装置６００は、ライセンス１１０の利用条件１１４からメタデータの編集可否情報を取得し、“メタデータ編集可能”または“メタデータ編集不可”のいずれかを判定する。メタデータの編集可否情報が“メタデータ編集不可”の場合は、暗号化コンテンツ３１０のコンテンツＩＤ３１１をメタデータ本体４１１に含むメタデータ４１０は編集不可である。メタデータの編集可否情報が“メタデータ編集可能”の場合は、ユーザ操作に従い、暗号化コンテンツ３１０のコンテンツＩＤ３１１をメタデータ本体４１１に含むメタデータ４１０を編集し、編集したメタデータ４１０を含む再デジタル署名要求を、メタデータ署名者ＩＤ４１２の署名者に送信し、メタデータ署名者ＩＤ４１２の署名者が再デジタル署名したメタデータ４１０を受信する。

【００９０】

尚、本実施の形態では、編集可否情報が“メタデータ編集可能”または“メタデータ編集不可”のいずれかを示すフラグであるが、編集可能なメタデータ４１０のメタデータＩＤであってもよい。この場合、編集可否情報で指定されたメタデータ４１０のみが編集可能と判定される。

同様に編集不可なメタデータ４１０のメタデータＩＤであってもよい。この場合、編集可否情報で指定されたメタデータ４１０のみが編集不可と判定される。

【００９１】

尚、本実施の形態では、メタデータ４１０を編集後にメタデータ署名者ＩＤ４１２の署名者により再デジタル署名しているが、端末装置６００が公開鍵と、秘密鍵と、公開鍵証明書５１０を保有している場合、端末装置６００がメタデータ４１０にデジタル署名してもよい。

【産業上の利用可能性】

【００９２】

本発明に係るコンテンツ配信システム１は、コンテンツプロバイダ３００によりメタデータ４１０の利用を制御できるため、コンテンツプロバイダ３００が意図しない信頼性の低いメタデータを排除できるコンテンツ配信システムとして有用である。

【図面の簡単な説明】

【００９３】

【図１】本発明の実施の形態に係るコンテンツ配信システム１の全体の概略構成を示す図である。

【図２】本発明の実施の形態に係るライセンス１１０の構成を示す図である。

【図３】本発明の実施の形態に係るユーザ情報ＤＢ２０１のテーブル構成を示す図である。

【図４】本発明の実施の形態に係る暗号化コンテンツ３１０の構成を示す図である。

【図５】本発明の実施の形態に係るメタデータ４１０の構成を示す図である。

【図６】本発明の実施の形態に係る公開鍵証明書５１０の構成を示す図である。

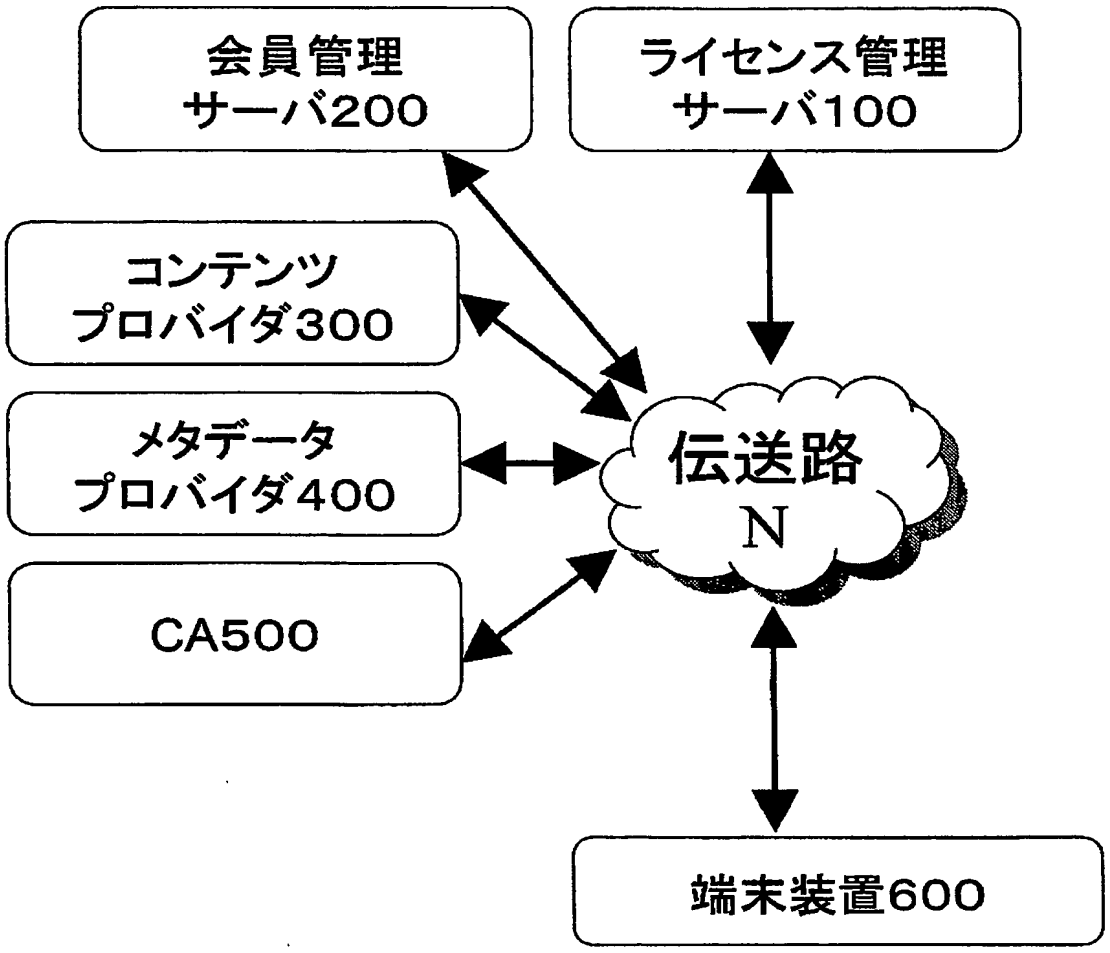
【図７】本発明の実施の形態に係るＣＲＬ５２０の構成を示す図である。
【図８】本発明の実施の形態に係るコンテンツプロバイダ３００またはメタデータプロバイダ４００が署名したメタデータの利用可否判定の処理を示すフローチャートである。
【図９】本発明の実施の形態に係るユーザが作成したメタデータの利用可否判定の処理を示すフローチャートである。
【図１０】本発明のコンテンツ配信システムの概略処理を示すフローチャートである。
【図１１】図８に示されるＩＤ比較（ステップＳ１０１）処理の詳細を示すフローチャートである。

【符号の説明】

【００９４】

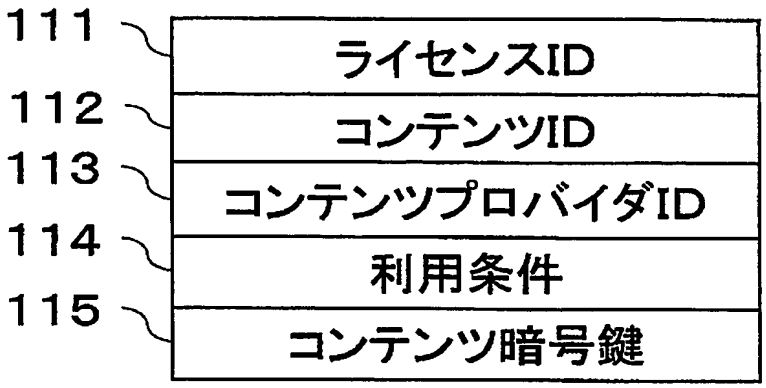
１　コンテンツ配信システム
１００　ライセンス管理サーバ
２００　会員管理サーバ
３００　コンテンツプロバイダ
４００　メタデータプロバイダ
５００　ＣＡ
６００　端末装置
１１０　ライセンス
１１１　ライセンスＩＤ
１１２　コンテンツＩＤ
１１３　コンテンツプロバイダＩＤ
１１４　利用条件
１１５　コンテンツ暗号鍵
２１０　ユーザ情報ＤＢ
２１１　ユーザＩＤ
２１２　ドメイン鍵
３１０　暗号化コンテンツ
３１１　コンテンツＩＤ
３１２　コンテンツプロバイダＩＤ
３１３　コンテンツ本体
４１０　メタデータ
４１１　メタデータ本体
４１２　署名者ＩＤ
４１３　デジタル署名
５１０　公開鍵証明書
５１１　主体者ＩＤ
５１２　主体者公開鍵
５１３　デジタル署名
５１４　署名者ＩＤ
５２０　ＣＲＬ
５２１　更新日時
５２２　リボークされた主体者ＩＤ

【書類名】図面
【図１】



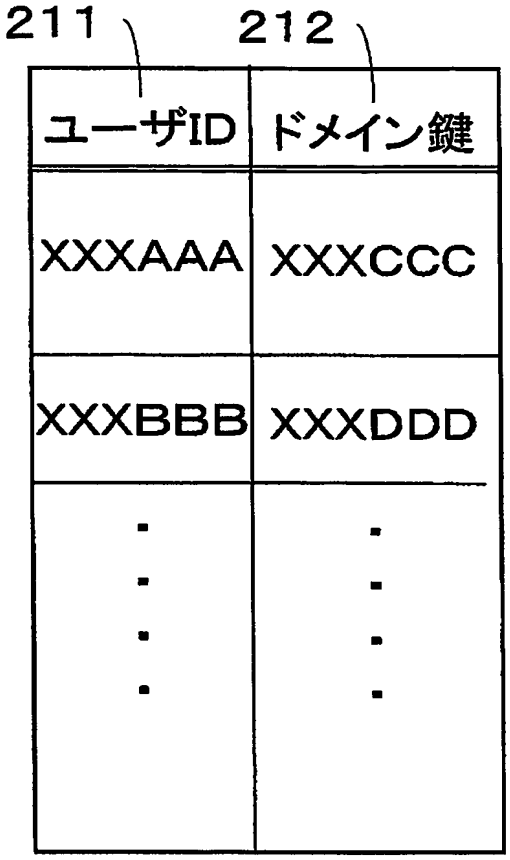

コンテンツ配信システム１

【図２】


111
ライセンスID
112
コンテンツID
113
コンテンツプロバイダID
114
利用条件
115
コンテンツ暗号鍵

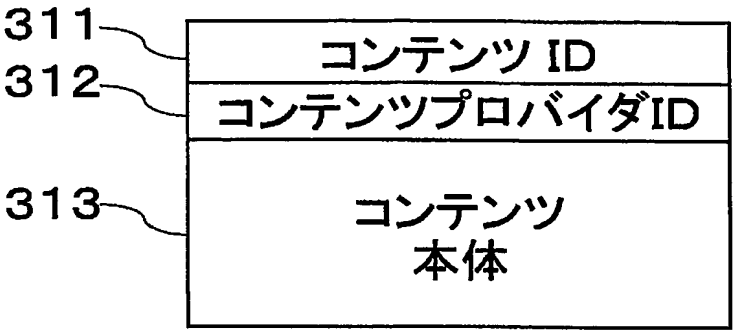
ライセンス１１０

【図３】



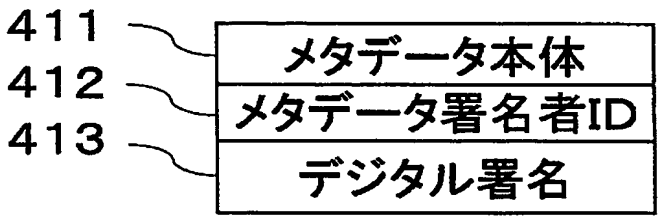

ユーザ情報DB　210

【図４】



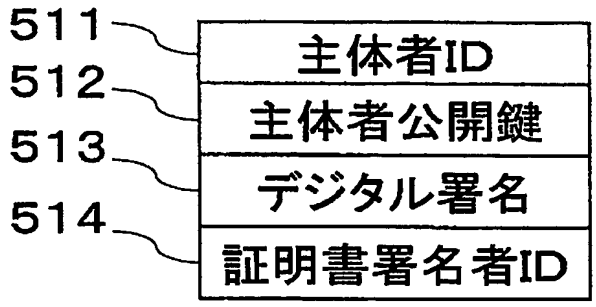

暗号化コンテンツ　310

【図５】



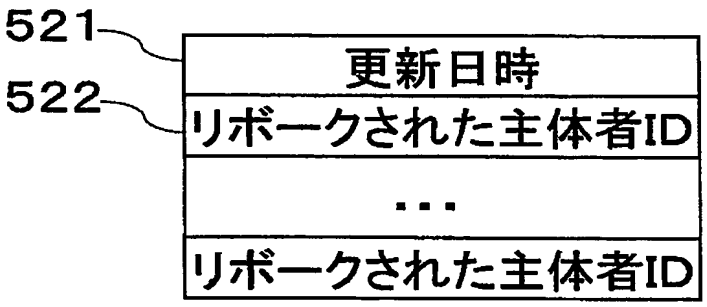

メタデータ　410

【図６】



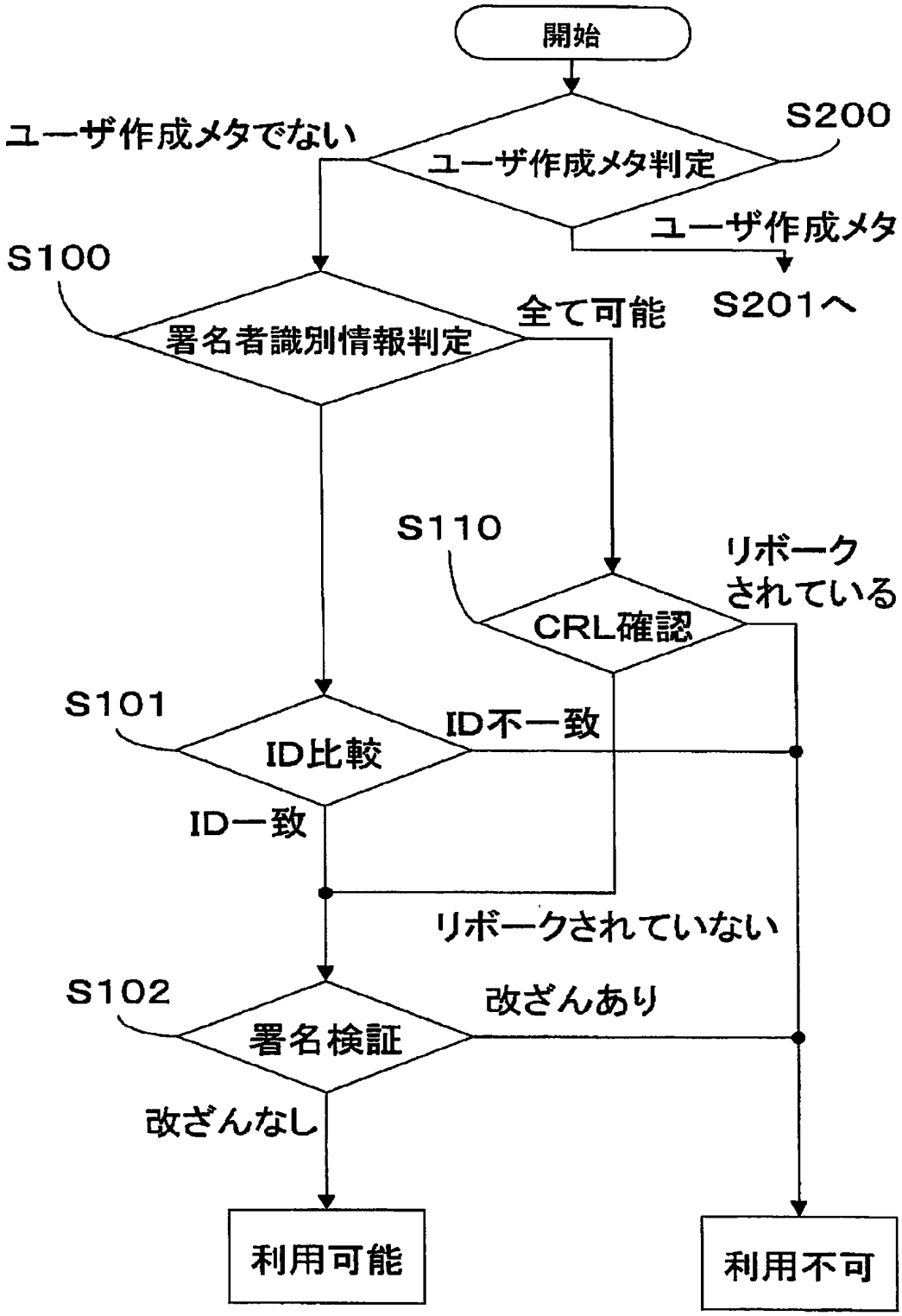

公開鍵証明書　５１０

【図７】

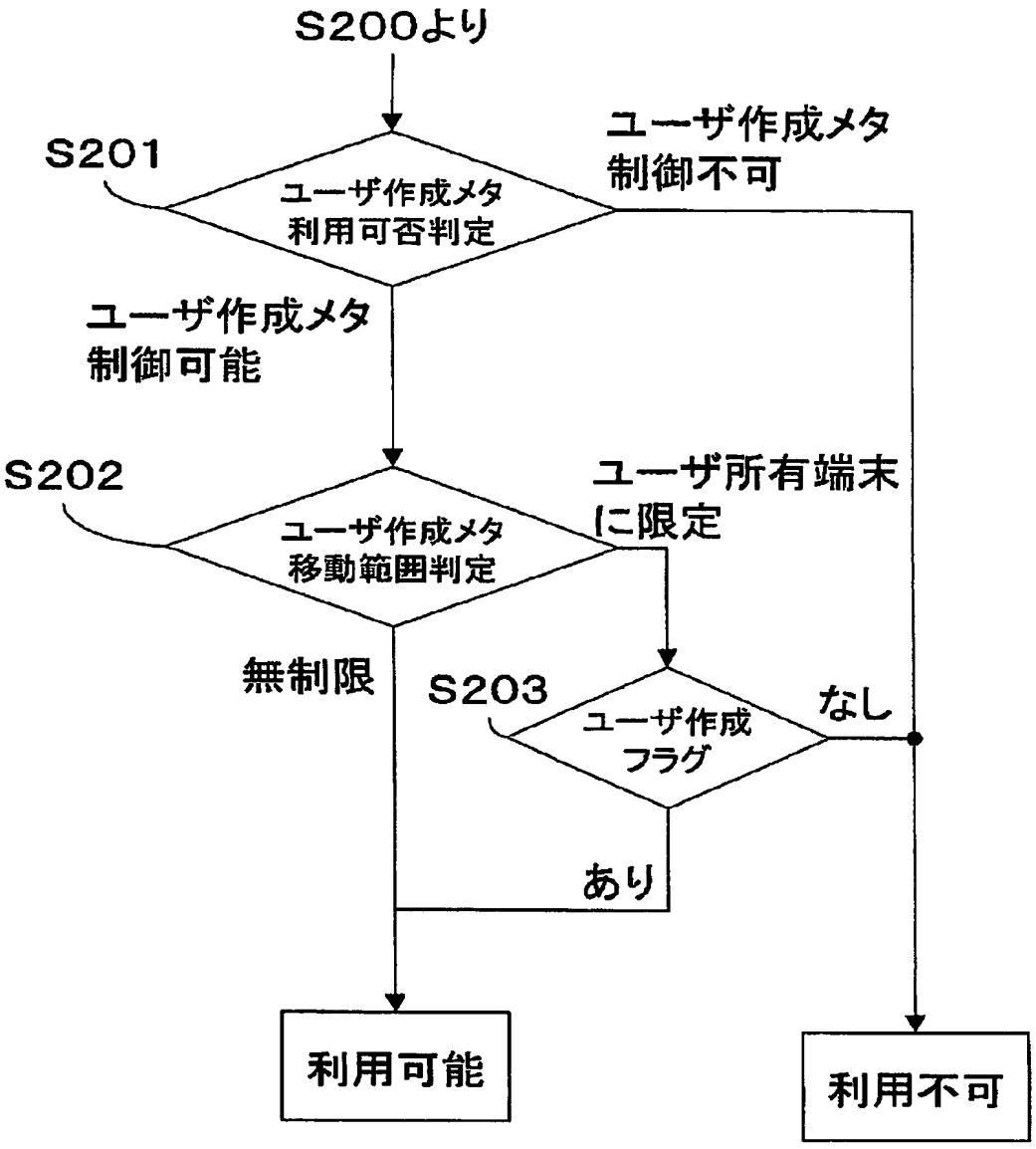



ＣＲＬ　５２０

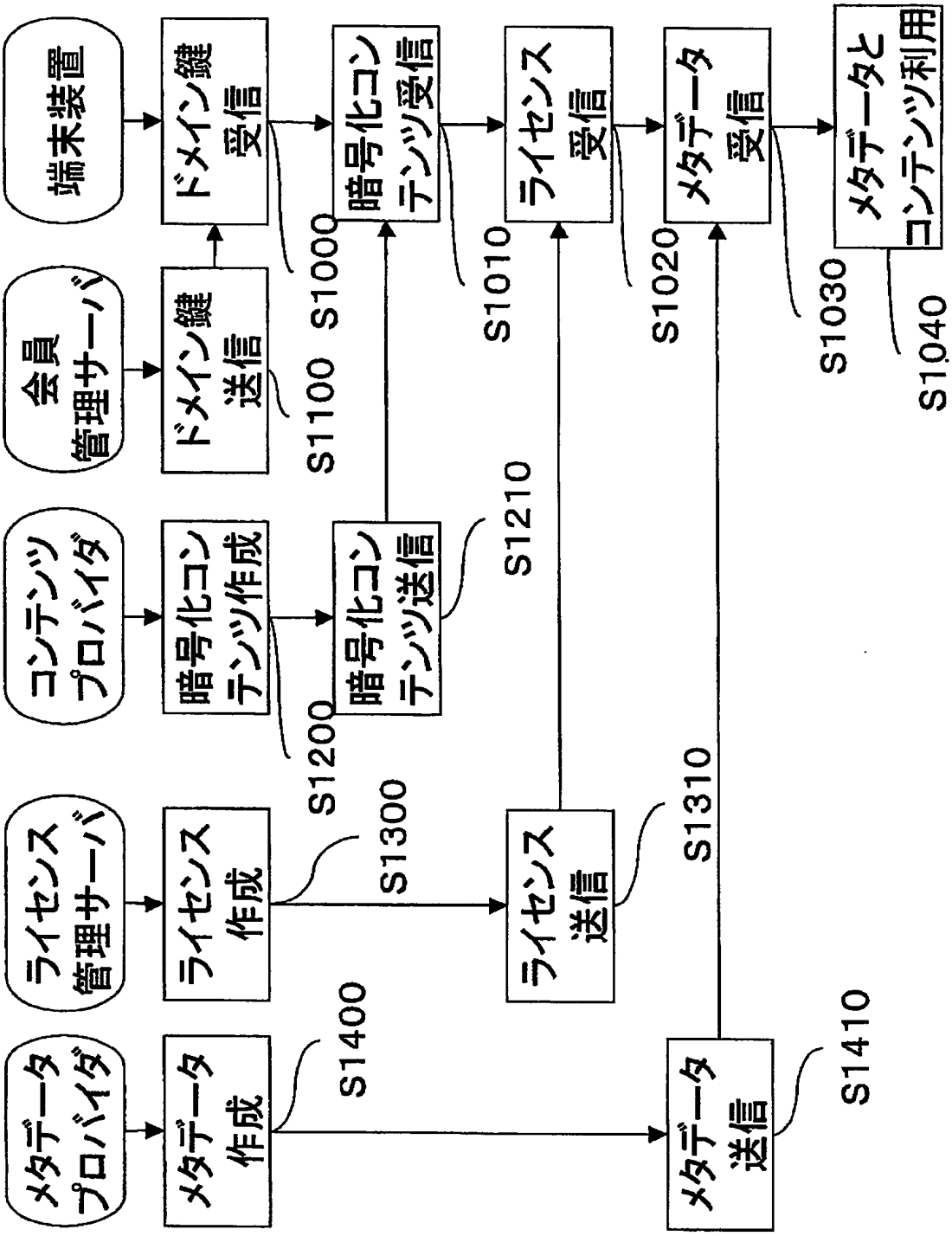
【図８】


開始
S200
ユーザ作成メタでない
ユーザ作成メタ判定
ユーザ作成メタ
S100
S201へ
全て可能
署名者識別情報判定
S110
リボーク
されている
CRL確認
S101
ID不一致
ID比較
ID一致
リボークされていない
S102
改ざんあり
署名検証
改ざんなし
利用可能
利用不可

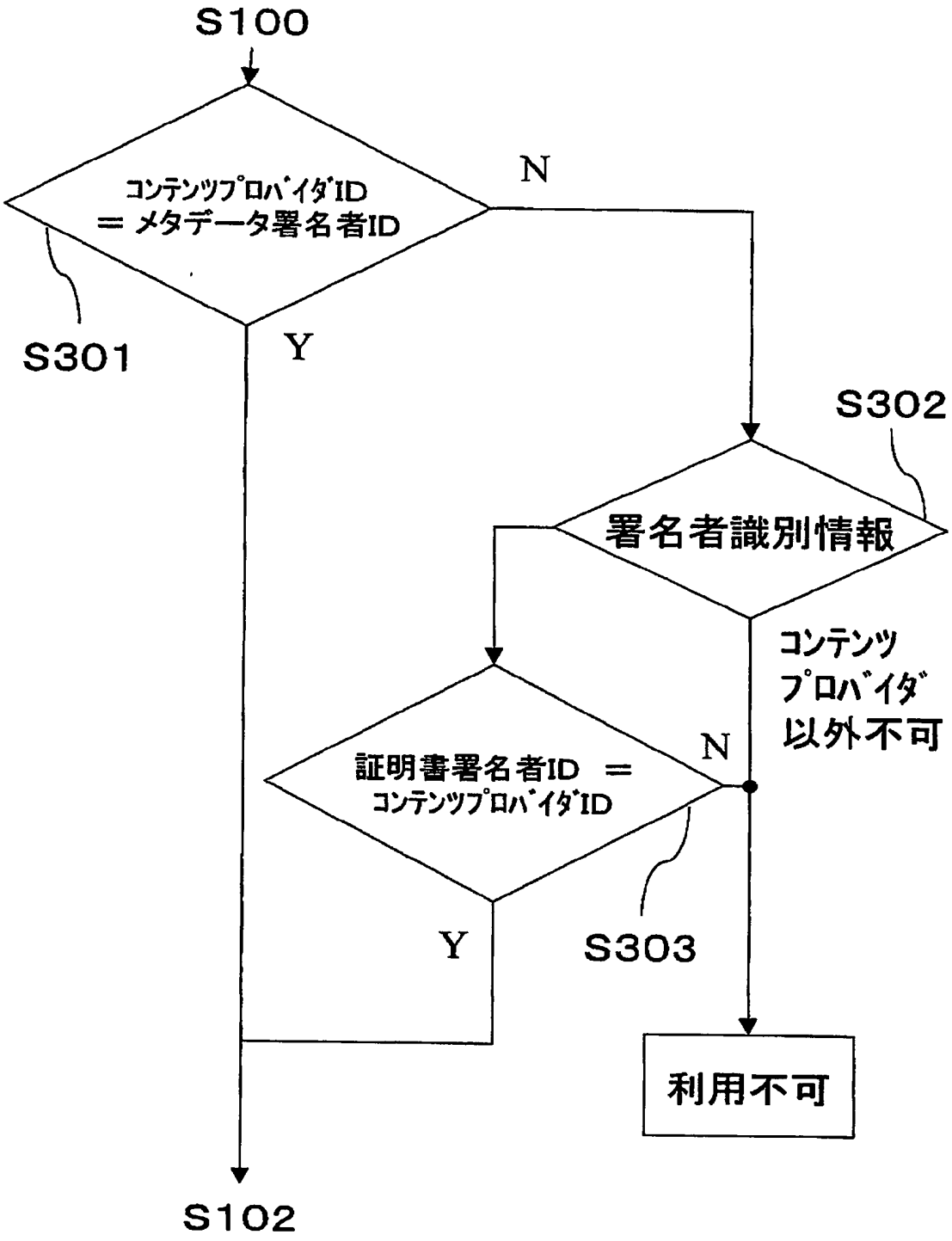
【図９】


S200より
S201
ユーザ作成メタ
利用可否判定
ユーザ作成メタ
制御不可
ユーザ作成メタ
制御可能
S202
ユーザ作成メタ
移動範囲判定
ユーザ所有端末
に限定
無制限
S203
ユーザ作成
フラグ
なし
あり
利用可能
利用不可

【図１０】


端末装置
会員管理サーバ
コンテンツプロバイダ
ライセンス管理サーバ
メタデータプロバイダ
ドメイン鍵受信
ドメイン鍵送信
暗号化コンテンツ作成
ライセンス作成
メタデータ作成
暗号化コンテンツ送信
ライセンス送信
メタデータ送信
暗号化コンテンツ受信
ライセンス受信
メタデータ受信
メタデータとコンテンツ利用
S1000
S1100
S1200
S1300
S1400
S1210
S1310
S1410
S1010
S1020
S1030
S1040

【図１１】


S100
コンテンツプロバイダID
＝メタデータ署名者ID
N
S301
Y
S302
署名者識別情報
コンテンツ
プロバイダ
以外不可
証明書署名者ID ＝
コンテンツプロバイダID
N
Y
S303
利用不可
S102

【書類名】要約書
【要約】
【課題】　コンテンツの提供者がデジタル署名したメタデータのみ利用可能なコンテンツ配信システムを提供する。
【解決手段】　端末装置６００は、署名者識別情報判定（ステップＳ１００）で、ライセンス１１０の利用条件１１４から取得した署名者識別情報が“コンテンツプロバイダ以外不可”の場合に、暗号化コンテンツ３１０から取得したコンテンツプロバイダＩＤ３１２とメタデータ４１０から取得したメタデータ署名者ＩＤ４１２をＩＤ比較（ステップＳ１０１）し、一致しない場合はメタデータ４１０を利用不可とする。
【選択図】　図８

# 認定・付加情報

| | |
|---|---|
| 特許出願の番号 | 特願２００３－３８０８４９ |
| 受付番号 | ５０３０１８６１５００ |
| 書類名 | 特許願 |
| 担当官 | 第七担当上席　　００９６ |
| 作成日 | 平成１５年１１月１２日 |

＜認定情報・付加情報＞

【提出日】　平成15年11月11日

特願２００３－３８０８４９

# 出願人履歴情報

識別番号　［０００００５８２１］

１．変更年月日　１９９０年　８月２８日
［変更理由］　新規登録
住　所　大阪府門真市大字門真１００６番地
氏　名　松下電器産業株式会社